3.1 Specifika zajišťování bezpečnosti

Mezi hlavní kategorie bezpečnostních technologií patří firewally, antivirové systémy, detekce narušení, správa zranitelností a správa obsahu stále více soustředěné do SIEM (Security Information and Event Management), tj. managementu bezpečnostních informací a událostí. Protože hrozby, jako jsou např. viry, trojské koně, malware, ransomware apod. mohou využít zranitelností IS v bránách, serverech nebo klientských sítích, musí být všechna tato řešení implementována v každé ze tří vrstev sítě.

Pokud není poskytnuta ochrana ve všech třech vrstvách systému, tj. datové (databázové), aplikační a prezentační, vzniká v informačním prostředí díra, kterou mohou hackeři, škodlivý SW, ale aktivní či pasivní činnost uživatelů, kompromitovat. To platí zejména pro prezentační vrstvu, na které jsou využívány osobní počítače, zde je nutné zajistit v v prezentační vrstvě byla důsledně řešena oprávněnost přístupu, kontinuální ochrana zpracovávaných dat a zálohování.

Nyní budeme podrobněji zkoumat různé bezpečnostní technologie a budou uvedeny základní postupy a přístupy ochrany podnikového informačního systému.

3.2 Zajištění a správa bezpečnostních nástrojů

Informační technologie zahrnují tři hlavní nástroje pro kontrolu přístupu k počítačovým i komunikačním systémům a pro omezení uživatelů při přístupu pouze k funkcím a činnostem odpovídajícím jejich potřebám v rámci nastavené úrovni autorizace, autorizace a správy účtů.

3.2.1 Autentizace

Autentizace je proces, který určuje, kdo jste, jaké máte oprávnění k přístupu k aplikacím, do informačního systému aj. Pro kontrolu a audit autentizačních procesů jsou v informačních systémech implementovány systémy řízení oprávněného přístupu (např. Active Directory v prostředí MS Windows).

Pokročilejší autentifikační technologie poskytují další bezpečnost během autentizačního procesu. Tyto technologie zahrnují použití fyzických zařízení nebo žetonů, jako jsou čipové karty, které uchovávají další informace k identifikaci daného uživatele. Také biometrické systémy mohou využívat jedinečné biologické vlastnosti, včetně otisků prstů nebo snímků sítnice, a ve stále větší míře používaného dynamického biometrického podpisu (DBP), aby byla dosažena vyšší úroveň autentizace, tzv. vícevrstvá autentizace.

Odborníci v oblasti bezpečnosti odkazují na nezbytnost minimálního použití dvou forem ověřování, tj. dvoufaktorové autentizace. Dvoufaktorová autentizace je doporučena pro řízení přístupu již ke standardním informačním systémům nebo pro vzdálený přístup k těmto systémům, neboť tímto způsobem je eliminována zranitelnost informačních systémů v případech využívání autentizace typu „jméno, heslo“.

Tradiční faktory ověřování můžeme rozdělit následovně:

- něco, co znáte, například heslo;
- něco, co máte, například symbol;
- něco, co jste, například biometrické charakteristiky;
- kde jste, například pomocí globálních satelitů pro určování polohy.

Klientská softwarová řešení mohou též využívat dalších nástrojů, jako jsou „tokeny" nebo "certifikáty", které jednoznačně identifikují jak vlastníka příslušné pracovní stanice (např. osobního počítače), tak i samotné fyzické zařízení. Toto SW řešení umožňuje řešit úskalí vzdáleného přístupu, kdy je ověřeno, že daný oprávněný uživatel přistupuje do systému z fyzického zařízení, které je deklarováno a je tak možné kontrolovat oprávnění k vzdálenému přístupu k systému i v rozsáhlých sítích. V každém případě by organizace a podniky by měly využívat dvoufaktorovou autentizaci pro přístup do systému, protože jednoduché uživatelské ID a hesla neposkytují dostatečnou záruku, že nedošlo k přístupu neoprávněných osob, zejména při nedostatečné správě hesel.

Problematika hesel, správa klíčů

Uživatelům musí být zaručeno, že mají jedinečné uživatelské ID a hesla pro přístup k počítačům, e-mailovým účtům a jiným informačním systémům. Identifikátory uživatelů a hesla jsou nejzákladnější formou ověřování (jak bylo uvedeno i nejzranitelnější) a jsou ekvivalentní „elektronickým klíčům“ k systémům a aplikacím. Tyto klíče musí být pečlivě kontrolovány, musí být zajištěna jejich správa (kontrola kvalitních hesel, jejich periodická obměna apod.), a uživatelé musí být poučeni, že při jejich zneužití platí presumpce viny – tj. daný uživatel je za zneužití daného „klíče“ zodpovědný.

Uživatelé musí dodržovat následující nejdůležitější povinnosti při práci s hesly:

1. Hesla nesmí být jakýmkoliv způsobem sdělena jiné osobě.
2. Hesla nesmí být nikde poznamenána a musí se udržovat v tajnosti.
3. Nesmí být, jakkoliv umožněno jiné osobě seznámit se s heslem.
4. Jako hesla nesmí být použita jména blízkých osob, zvířat a další slova, která mohou být odhadnuta ze znalosti držitele hesla, nebo neobsahovalo po sobě jdoucí stejné.
5. Heslo musí být dostatečně silné, tak aby se nedalo jednoduše strojově nebo ručně prolomit (kombinace velkých a malých písmen a číslic, délka alespoň 10 znaků) a mělo by být pravidelně měněno v závislosti rizicích spojených s prolomením.
6. Hesla nesmí být zaznamenána na papíře nebo v obdobné podobě (výjimku tvoří bezpečné uložení administrátorských hesel pro případ havárií).

Hesla se musí změnit v případě jakéhokoliv náznaku možného kompromitování systému nebo hesla. Plnění těchto požadavků nelze nechat na samotných uživatelích, je nutno implementovat do informačních systémů řešení, které řádnou správu hesel vynucovat.

3.2.2 Autorizace

Funkce autorizace umožňuje správcům systému omezit některé speciální oprávnění na určité role nebo funkce, které zaměstnanci vykonávají v rámci organizace. S využitím autorizace je tak řešeno strukturování oprávnění jednotlivých uživatelů informačního systému. Například všichni uživatelé v dané společnosti mohou mít e-mailový účet pro všeobecné použití, ale pouze omezený počet zaměstnanců by měl privilegovaný přístup k definovaným aplikacím. V tomto případě systém umožňuje administrátorovi systému, aby zajistil kontrolu určitých omezených funkcí.

Jiným příkladem jsou systémy s jednotlivými aplikacemi, ve kterých jsou odděleny typy povinností a pravomocí dle dané role jednotlivých uživatelů. Např. personál, který má přístup k citlivým informacím, (například mzda).

Správa autorizačních oprávnění musí zjistit, kdo přistupuje k vymezeným systémům a jaké činnosti zde provádí. Musí být navržen systém pravidelného provádění vnitřních auditů, pro kontrolu, že nikdo nepřistupuje k systémům bez řádné autorizace nebo se záměrem nevhodného použití.

Například všichni zaměstnanci v dané finanční oblasti mohou být oprávněni k přístupu do systému plánování podnikových zdrojů (ERP) společnosti. Pokud ovšem auditor zjistí, že zaměstnanci používají systém v době mimo provozní dobu bez přítomnosti supervizorů, může být nezbytné provést další šetření, aby se zajistilo, že tyto činnosti jsou vhodné.

Správa účtů

Správa uživatelských účtů ve více systémech je obtížná úloha a software pro jednotné přihlášení je součástí řešení tohoto problému (Single Sign on – SSO). Tato řešení poskytují jediné ID uživatele a heslo pro přístup k více systémům, které mohou existovat v dané společnosti. SW pro přihlášení s jediným přístupem však přináší významné bezpečnostní zranitelnosti v případech, kdy jsou v podniku provozovány systémy s odlišnou architekturou. V těchto případech může SSO, které vytváří bezpečnější prostředí ve vztahu k uživatelům, způsobit rizika při implementaci do širokého spektra podnikových aplikací.

Správa účtů, jako třetí z nástrojů při řešení přístupu, slouží jak k auditu, a tak i kontrole využití zdrojů. Z pohledu auditu je důležité mít dobré znalosti o tom, kdo přistupuje k různým zdrojům v rámci podniku a mít přehled o činnosti uživatelů. Tento přístup spadá do „dobré praxe“, vyžadované při revizi protokolů kritických systémů (nejenom), aby bylo zajištěno, že k nim mají přístup pouze oprávnění uživatelé.

Správa účtů je těsně spojena s autorizací, kdy základem je pravidelná kontrola uživatelů, kteří mají přístup do vyhrazených oblastí, jako je datové centrum podniku apod. Navíc je nutnou podmínkou při vytváření prostředí, kde lze zajistit dohledání o činnostech s příslušnými informacemi (daty, elektronickými dokumenty) v celém jejich životním cyklu.

3.2.3 Šifrování

Šifrování je proces převodu dat do formátu, který neoprávněná osoba (ale i oprávněná osoba bez znalosti použitého klíče) nemůže snadno přečíst.

Existují dvě hlavní formy moderního šifrování: symetrické a asymetrické.

Při symetrickém šifrování používají obě strany stejný tajný klíč pro šifrování a dešifrování zpráv. Jedná se o bezpečnější a rychlejší způsob šifrovaní dat. Velkou nevýhodou tohoto způsobu je obtížná distribuce tajných klíčů, zejména v rozsáhlých systémech či sítích.

Asymetrické šifrování nevýhodu distribuce tajných klíčů v rozsáhlých systémech či sítích efektivně odstraňuje. V daném případě každá strana má veřejný klíč pro šifrování a privátní klíč pro dešifrování dat. Při asymetrickém šifrování odesílatel zprávy použije veřejný klíč příjemce s cílem zašifrovat zprávu pro něj. Příjemce této zprávy použije svůj privátní klíč k dešifrování této zprávy. Veřejný klíč nelze požít dešifrování zprávy ani k tomu, aby z něj rekonstruoval privátní klíč příslušného příjemce. I u asymetrického šifrování vyvstávají problémy s „klíčovým hospodářstvím“.

Je třeba zajistit, že:

- příslušný veřejný klíč patří deklarovanému uživateli;
- privátní klíč je bezpečně uložen, tak aby nedošlo k jeho zneužití.

V případě, že není ověřena jednoznačná vazba mezi uživatelem a jeho veřejným klíčem může dojít k narušení důvěrnosti dat, nebo nelze spoléhat na autenticitu dat. Proto účastníci komunikace nedistribuují veřejné klíče sami, ale využívá, tzv. certifikátů vydávaných nezávislými třetími stranami – certifikačními autoritami. Účastnící komunikace tak při přenosu dat využívají certifikátů - tj. potvrzení že daný veřejný klíč patří příslušnému subjektu.

S touto problematikou souvisí PKI (Public Key Infrastructure) tj. infrastruktura veřejných klíčů, kterou vytváří technické prostředky, organizační opatření a administrátoři, s cílem zajistit správu certifikátů veřejných klíčů. Využitím systému PKI lze pak zajistit důvěryhodnost elektronických identit.

Základem PKI je certifikační autorita vydávající certifikáty a seznam zneplatněných certifikátů (CRL Certificate Revocation List), které odpovídají standardu X.509. Certifikační autorita, jako vydavatel certifikátu je odpovědná za to, že certifikát k asymetrickým klíčům je vydán autentizovanému držiteli těchto klíčů, a tak je garantována platnost jednotlivých uživatelů.

První systémy PKI využívaly služeb jedné tzv. kořenové certifikační autority, která vytvářela proprietární certifikáty. V současné době musí být vydávané dokumenty v souladu s normami, což v praxi znamená, že možné vytvářet různé modely PKI od podnikových až po PKI postavené kolem certifikovaných certifikačních autorit.

K ochraně přenášených e-mailových zpráv se využívá protokol S/MIME, který využívá jak asymetrické, tak symetrické šifrování) a protokol Secure Sockets Layer (SSL), který je součástí protokolu HTTPS.

V kapitole jsou uvedeny hlavní aspekty při zajišťování bezpečnosti v informačních systémech. Jsou zde rozebrány základní typy bezpečnostních nástrojů. Samostatná část je věnována problematice šifrování.

1. Jaké bezpečnostní nástroje a metody se využívají při zajištění přístup do informačního systému?
2. Jaký je rozdíl mezi autentizací, dvoufaktorovou autentizací a autorizací?
3. Co je důležité dodržovat při správě hesel a klíčů?
4. Jaké jsou metody šifrování?

Literatura k tématu:

[1] CLARK, David, Leon. *Enterprise Security: The Manager's Defense Guide,* Addison-Wesley Professional, 2003, ISBN 780201719727, Počet stran: 264.